The HIPAA Implementation Newsletter
Issue #36 – June 14, 2002
| Security |
Web format with links at http://lpf.com/hipaa

Periodically, we find that most of the information we have gathered for the newsletter relates to security. Partly, that is a normal progression. Issues related to transactions, code sets and privacy have been addressed early because they have the earliest deadlines and are defined by final rules. Partly, it is because of the three C's of security: complexity, cost and change. This issue is all about security. We'll have additional things to report in the next issue.

___Security: Expense or Investment?___

Consulting Magazine has recognized Rudolph Giuliani, former mayor of New York, as the most influential consultant of the year. We find his perspective on planning and security useful and relevant to HIPAA implementation:

CM: What is it that CEOs need to better understand about security and crisis planning?
Giuliani: From talking with CEOs, what we know is that while they understand there's a security problem, they often feel that the time they spend on their security problem is wasted because they think it's not about making money. But the way I look at this is that I ran a very large, complex corporation - New York City had a $40 billion budget, 50 different subgroups or affiliated entities that did all different types of work, and we did a lot of crisis management preparation. We did tabletop exercises, and we always asked the question what was the worse thing that can happen to us and are we ready for it, and what I found in my own experiences as a CEO was that all of this helped us in the management of the business by revealing some of things that we were doing wrong day-to-day. ... So far, the CEOs we've done this with are today convinced of the second benefit, where you start to see some of the other problems that exist in your business and you start to run it day-to-day more efficiently.

CM: How do your security consulting offerings differ from those of other consulting firms?
Giuliani: … the fact that we can integrate [security planning] into the running of your business and make it work day-to-day. ... In the past, the way people approached security was as a separate, segregated aspect of their business. It was something that was either necessary or not, and almost thought of as a loss leader. It was something "we have to do," but with little thought given to how it could actually help make businesses more profitable. I think we can show people how to do that.

CM: You've suggested that planning for one crisis might help you with another.
Giuliani: Yes. … after the millennium was over, I sat around with my deputy mayors and budget directors and felt a little guilty and said: "Gosh, why did we spend so much money on this?" And then, when September 11 happened, I realized within a few days how valuable it was that we had done all the

work. … by having thought our way through Y2K, we were prepared for the September 11 crisis, and that's what proper security and crisis management can do for you. You may not plan for the correct crisis, but if you have planned for a crisis you can handle nearly anything that's going to happen to you.
Excerpt from Consulting Magazine
+ More at: http://www.consultingcentral.com/features/06_02/coverstory.html

~=~=~=~=~=~=~=~=~=~=~=~=~=~=~
On July 2, we will be asking and answering the questions: What is HIPAA? and What do you need to know? in an online event produced by SearchSecurity at 01:00 PM EDT. This will be a high level presentation that may be of interest to some of your associates.
+More at:
http://searchsecurity.techtarget.com/onlineEvents/0,289675,sid14,00.html
~=~=~=~=~=~=~=~=~=~=~=~=~=~=~

___Security: Reducing Insider Attacks___

"Most computer attacks come from the outside. But the costliest ones come from the inside. Here's how to manage the risk without making honest employees feel like crooks.

"Many companies don't do enough to protect against insider threats because they are leery of breaking the trust they have built with their employees. Treat someone like a criminal, the thinking goes, and he might start to act like one. The good news is that there are some easy ways to improve internal security without making honest people feel like crooks—steps that will help protect against external threats as well. Here are five things you can do.

"Emphasize Security from Day One: Good security starts with whom you hire, and that's why it's crucial to have a preemployment screening, including reference checks [tailored to the person's job and career path.] CIOs can also limit the damage any one employee can do by setting up access controls that map a person's job function to the resources he needs to do that job. Do that from day one, [or in the case of HIPAA, do it throughout the organization] and your company can avoid giving the impression that access levels have to do with him as a person—they're simply part of a given job function.

"Build Security from the Inside Out: These access controls are only the first step toward a decreasing emphasis on what's known as perimeter protection—security's equivalent of the moat around a castle. Some corporations run hard on the outside and soft on the inside: Once you get in, you have free access.

"Make Security Part of the Culture: Another key element is establishing a culture that values security. That helps keep the honest people honest and makes it easier to deal with people who cross the line. CIOs who decide to implement stricter policies for employees should be doubly sensitive to educating users about reasons for the changes. "This is a classic situation where what your culture is and what you've done in the past lays a

foundation for future efforts," says Mitchell Marks, an organizational psychologist in San Francisco. "If you don't explain why you are [increasing security], then people will talk about it at the coffee machine, fill in the information voids with perceptions that are probably more negative than reality [and conclude]: Leadership doesn't trust us."

"Watch for Unusual Activity: … look at what's happening on your company's network—a high number of FTP downloads, for example, or unusual activity in a department that is going through a painful reorganization, or even e-mails that match keyword searches.

"Know How to Let Go: A little sensitivity when someone leaves the company can go a long way in avoiding retaliation or sabotage. But there are technical details to take care of as well. It can take months for IT departments to painstakingly close the accounts of a former employee because of poor communication with HR or because there are so many different accounts controlled by different systems administrators, which is a major problem not only because employees might attempt to access system resources but also because hackers can take advantage of inactive accounts. … when someone leaves our IT department under suspect circumstances, we go back and review the program changes that person has implemented recently."
+ More at: http://idg.net/ic_874030_4394_1-1681.html

___Security: CSO and CTO? Security Moves Up the Corporate Ladder___

A recent article from the McKinsey Quarterly, says: "Although information security has traditionally been the responsibility of information technology departments, some companies have made it a business issue as well as a technological one. ...
But most companies continue to view information security as a technological problem calling for technological solutions--even though technology managers concede that today's networks cannot be made impenetrable and that new security technologies have a short life span as hackers quickly devise ways around them.

"Delegating security to technologists also ignores fundamental questions that only business managers can answer. … One online retailer, Egghead.com, lost 25 percent of its stock market value in December 2000, when hackers struck its customer information systems and gained access to 3.7 million credit card numbers. Egghead, of course, had security systems in place and claimed that no data were actually stolen, but it lacked the kind of coordinated organizational response necessary to convince customers and shareholders that their sensitive data were actually secure. [COMMENTARY: The perception of security that is created by the way a problem is handled will have an impact on the organization, its affiliated professionals and its financial supporters. Security must extent from minimizing the risk of an incident through mitigation if there is one.]

"… CSOs at best-practice companies have the clout to make operational changes... Only the CEO can overrule the CSO--and rarely does. In the typical company, by contrast, a security manager in the IT unit has responsibility for security but little power to effect broader change in the

system. In addition, CSOs at best-practice companies conduct rigorous security audits, ensure that employees have been properly trained in appropriate security measures, and define procedures for managing access to corporate information.

"The role of information security, and of the chief security officer, varies by industry, the value of a company's data, and the intensity of the regulatory requirements it faces. At a health care organization, to give just one of many examples, the loss or alteration of records about patients could cause injury or death--an avoidable and therefore absolutely intolerable risk.

"Today, most business leaders pay as little attention to the issue of information security as they once did to technology. ... In a networked world, when hackers steal proprietary information and damage data, the companies at risk can no longer afford to dismiss such people as merely pesky trespassers who can be kept at bay by technological means alone.
+ More at:
http://www.mckinseyquarterly.com/article_page.asp?ar=1192&L2=13&L3=13

___Security: Tracking HIPAA Security Progress___
We debated including a long checklist, but we found ourselves acknowledging items we hadn't thought of and adding our own ideas. We also found it a good measure of progress.

"… provider and payer organizations must implement significant portions of the security rule--final or not--to fully comply with the privacy rule, which has an April 14, 2003, deadline. "You can have security without privacy, but you cannot have privacy without security," says Thomas Walsh, principal consultant at CTG HealthCare Solutions. He gave attendees a HIPAA Security Readiness Scorecard that lists 36 tasks, with checkmarks designating which tasks should be completed now and which should be in progress.

What should be completed by now:
* Designate a security officer or manager.
* Communicate the security officer designation to the workforce.
* Appoint a HIPAA project manager.
* Appoint a cross-functional HIPAA project steering committee.
* Establish HIPAA subcommittees for the transactions and code sets, privacy and security rules.
* Conduct a HIPAA readiness assessment.
* Inventory polices and procedures for privacy and security.
* Inventory information systems and the criticality/sensitivity of the information processed.
* Inventory business associates who handle protected information.
* Inventory biomedical equipment that stores protected information.
* Inventory employees with remote access to patient information systems.
* Inventory vendors with remote access to patient information systems.
* Solicit HIPAA readiness plans from information systems vendors.
* Develop a HIPAA compliance plan, budget and reporting system.
* Conduct workforce HIPAA awareness sessions.

What should now be in progress?
* Create new policies, procedures and forms identified through the readiness assessment, including incident response.
* Further develop and confirm the corporate risk profile.
* Conduct a risk analysis based on the readiness assessment.
* Develop or update contingency and disaster recovery plans.
* Establish a facility security plan for safeguarding patient information.
* Implement destruction policies for trash and other media containing protected information.
* Adopt backup, storage and retention procedures for all media containing protected information.
* Establish and document formal security and privacy training programs.
* Determine actions or items to be audited, adopt an audit trail retention policy, and establish and conduct an audit trail monitoring process.
* Define minimum security standards for information systems that store or process protected information.

A number of initiatives for a comprehensive HIPAA security compliance program follow after completion of the above projects, according to Walsh. They include:
* Create guidelines on workstation use and location.
* Establish a formal configuration/change control process, including anti-virus updates.
* Review access controls and consider creating a role-based model.
* Automate the process of notifying I.T. staff of terminations and transfers.
* Implement HIPAA language for chain of trust agreements.
* Conduct a vulnerability scan on information systems that store or process protected information.
* Certify information systems that store or process protected information.
* Conduct a network intrusion test.
* Test incident response.
* Review the information security program.
* Test contingency and disaster recovery plans.
http://www.healthdatamanagement.com/html/news/NewsStory.cfm?DID=8674

___HIPAA Conferences___

The Centers for Medicare & Medicaid Services has announced the planned broadcast of "Meeting the HIPAA Challenge: Implementing the HIPAA Standards and the Administrative Simplification Compliance Act." This program will be a satellite broadcast and Webcast. The Webcast will be available for 90 days after the initial broadcast, which will occur on June 18, 2002, from 2:00-3:30 P.M. (EDT).
+ More at: http://www.hcfa.gov/medlearn/broadcst.htm

HIMSS of Southern California June program, "CIO Forum and Legislative Update" June 28, Long Beach CA, 8:00 am to 1:30 pm
+ Info: maggie.mcdaniel@huntingtonhospital.com

Emerging Technologies and Healthcare Innovations Congress – ETHIC 2002 June

19-21, 2002 Washington D.C. Includes a HIPAA Compliance track
http://www.ethic2002.com/events/show.asp?showid=70&mn=1.1

"HIPAA -- What it is, and what you need to know" Online event Jul 02, 2002 at 01:00 PM EDT (17:00 GMT) Speaker: Hal Amens, is the President of Lyon, Popanz & Forester and the publisher of this newsletter.
+More at:
http://searchsecurity.techtarget.com/onlineEvents/0,289675,sid14,00.html

The HIPAA Colloquium at Harvard University, August 19 - 23, 2002 in Cambridge, MA, www.HIPAAColloquium.com

The fifth National HIPAA Summit, October 30 - November 1, 2002 in Baltimore, MD, www.HIPAASummit.com .

_____

To be removed from this mail list, click:
mailto:hipaa@lpf.com?subject=remove
To subscribe, click: mailto:hipaa@lpf.com?subject=subscribe We appreciate it if you include information about your firm and your interests.

Information in the HIPAA Implementation newsletter is based on our experience as management consultants and sources we consider reliable. There are no further warranties about accuracy or applicability. It contains neither legal nor financial advice. For that, consult appropriate professionals.

Lyon, Popanz & Forester http://lpf.com is a management consulting firm that designs and manages projects that solve management problems. Planning, and project management for HIPAA are areas of special interest.